

Agenda

Présentation de la mission

TP



Cours Audit des SI >> TP 5 >> 25.11.2005

Audit des ordinateurs portables

Présentation de la mission

- L'entreprise TOUBUREAU fait appel à vos services pour auditer son parc d'ordinateurs portables. Actuellement, les commerciaux (5) et le DG (1) utilisent des laptops. Ces laptops sont destinés à la saisie des commandes chez les clients. Les commerciaux possèdent l'historique complet de leurs clients alors que le DG possède l'historique de tous les clients. Les données sont considérées comme très sensibles par la société.
- Chaque soir les commerciaux envoient les informations par e-mail à la société. Le matin, ils reçoivent un e-mail pour actualiser leurs données. Les données des e-mails sont traitées automatiquement par le logiciel VENTI.
- Le DG craint qu'un commercial indélicat puisse quitter la société avec des données sensibles. En outre, un article de PME Magazine l'a convaincu que la sécurité des laptops était très largement sous-estimée au sein de TOUBUREAU.

Mémo du responsable informatique au DG

- 6 laptops ThinkPad X41
- Configuration BIOS d'origine
- Configuration WindowsXP d'origine
- Ne sont pas intégrés dans l'Active Directory car il y a des problèmes de droits trop restrictifs sur les profiles de l'AD
- Réseau configuré avec DHCP
- Les mises à jour sont effectuées par le responsable informatique quand les commerciaux sont au bureau (environ 6x par an)



Travail à réaliser

- Faire une liste des risques qui s'appliquent à cet audit
- Choisir 2 objectifs de contrôle du domaine DS et les appliquer à la situation de TOUBUREAU. Préparer les recommandations en découlant.

Laptop Security Guidelines

- **Basic Security Measures**
 - Choose a secure operating system and lock it down
 - Enable a strong BIOS password
 - Asset Tag or Engrave the laptop
 - Register the laptop with the manufacturer
- **Physical Security**
 - Get a cable lock and use it
 - Use a docking station
 - Lock up your PCMCIA cards
 - Use a personal firewall on your laptop
 - Consider other devices based on your needs
 - Use tracking software to have your laptop call home

Laptop Security Guidelines (suite)

- **Protecting your Sensitive Data**
 - Use the NTFS file system
 - Disable the Guest Account
 - Rename the Administrator Account
 - Consider creating a dummy Administrator account
 - Prevent the last logged-in user name from being displayed
 - Enable EFS (Encrypting File System)
 - Disable the Infrared Port on you laptop
 - Backup your data before you leave
 - Consider using offline storage for transporting sensitive documents
- **Preventing Laptop Theft**
 - No place is safe
 - Use a non descript carrying case
 - Beware of payphones...
 - When traveling by air....
 - When traveling by car...
 - While staying in a hotel...
 - When attending conventions and conferences...
 - Make security a habit

<http://labmice.techtarget.com/articles/laptopsecurity.htm>